



NCSC-2025-0147

Kwetsbaarheden verholpen in F5 BIG-IP

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 09-05-2025

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

F5 heeft kwetsbaarheden verholpen in de BIG-IP systemen.

Duiding

De kwetsbaarheden bevinden zich in verschillende configuraties van de BIG-IP systemen, waaronder het Traffic Management Microkernel (TMM) dat kan worden beëindigd door ongepubliceerde verzoeken. Dit kan leiden tot prestatie- en stabiliteitsproblemen, vooral voor softwareversies die End of Technical Support (EoTS) hebben bereikt. De kwetsbaarheden kunnen ook leiden tot ongeautoriseerde toegang en privilege-escalatie voor gebruikers, wat de beveiliging van de systemen in gevaar kan brengen.

Oplossingen

F5 heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://my.f5.com/manage/s/article/K000139503>
- <https://my.f5.com/manage/s/article/K000140968>
- <https://my.f5.com/manage/s/article/K000150668>
- <https://my.f5.com/manage/s/article/K000140937>
- <https://my.f5.com/manage/s/article/K000137709>
- <https://my.f5.com/manage/s/article/K000150598>
- <https://my.f5.com/manage/s/article/K000140574>
- <https://my.f5.com/manage/s/article/K000139571>
- <https://my.f5.com/manage/s/article/K000140919>
- <https://my.f5.com/manage/s/article/K000149952>
- <https://my.f5.com/manage/s/article/K000148591>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-35995	8.7 HIGH
➤ CVE-2025-36504	8.7 HIGH
➤ CVE-2025-36525	8.7 HIGH

> CVE-2025-36546	9.2 CRITICAL
> CVE-2025-36557	8.7 HIGH
> CVE-2025-41399	8.7 HIGH
> CVE-2025-41414	8.7 HIGH
> CVE-2025-41431	8.7 HIGH
> CVE-2025-41433	8.7 HIGH
> CVE-2025-46265	8.7 HIGH
> CVE-2025-31644	8.5 HIGH

CWE's

CWE	Beschrijving
> CVE-125	Out-of-bounds Read
> CVE-404	Improper Resource Shutdown or Release
> CVE-476	NULL Pointer Dereference
> CVE-770	Allocation of Resources Without Limits or Throttling
> CVE-863	Incorrect Authorization
> CVE-787	Out-of-bounds Write
> CVE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
> CVE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')

Getroffen producten

F5
BIG-IP

BIG-IP Next
BIG-IP Next CNF
BIG-IP Next SPK
F5OS - Appliance
F5OS - Chassis

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.